REMARKS

The Present amendments and remarks are submitted in accompaniment of a request for continued examination. Claims 1-3, 5-24, 26-28, 50-51 and 53-68 are pending in the present application. Claims 1-3, 5, 6, 11-20, 22, 26-28, 50, 51 and 53-55 have been amended. Claim 52 has been cancelled. New claims 57-68 have been added.

The amendments to claims 1-3, 5, 6, 11-20, 22, 26-28, 50, 51 and 53-55, and the addition of new claims 57-68 are supported in the as-filed specification and drawings. For example, the amendments to claims 1, 3, 11, 12, 14, 19, 20, 22, 26, 50 and 51 find support in at least paragraphs [0038] and [0039] of the published specification. Similarly, Applicants assert that support for new claims 57-68 is found in paragraphs [0039]-[0041]. Furthermore, Applicants believe that the cancellation of claims 29-49 in a previous response results in no additional fees for the addition of new claims 57-68.

Claim Rejections – 35 USC § 101

The Office Action rejected claims 14-21 under 35 U.S.C. §101 because the claims are alleged to be directed to non-statutory subject matter since the specification "defines the means to include software **only** [0064]." The Examiner continues to assert that merely because the specification mentions "software" in paragraph [0064] that this makes claims 14-21 non-statutory subject mater. Applicants note that the Examiner has failed to provide any support explaining how means for outputting the second private key and means for outputting the first public key, as recited in claim 14, or means for receiving a first public key and means for receiving a second public key from a mobile user device, as recited in claim 19, could be accomplished without hardware. However, in the interest of moving the prosecution of the present application forward, Applicants have amended claim 14 to recite "means for storing the first private key at the mobile user device," and claim 19 to recite "means for storing the first public key and the second public key." Applicants assert that such elements clearly overcome any reasonable rejection under 35 U.S.C. §101.

Accordingly, Applicants respectfully request that the Examiner withdraw the rejection of claims 14-21 under 35 U.S.C. §101.

Claim Rejections – 35 USC § 103

The Office Action rejected claims 1-3, 5-24, 26-28, 50, 51 and 53-56 under 35 U.S.C. §103(a) as being allegedly obvious over U.S. Patent No. 5,761,306 (hereinafter "Lewis") in view of U.S. Patent No. 6,009,177 (hereinafter "Sudia").

These rejections are respectfully traversed in their entirety.

The Office has the burden under 35 U.S.C. § 103 to establish a prima facie case of obviousness. *In re Piasecki*, 745 F.2d 1468, 1471-72, 223 USPQ 785, 787 (Fed. Cir. 1984). To establish a prima facie case of obviousness, four basic criteria must be met. Obviousness is a question of law based on underlying factual inquiries, which inquiries include: (A) determining the scope and content of the prior art; (B) ascertaining the differences between the claimed invention and the prior art; (C) resolving the level of ordinary skill in the pertinent art; and, if applicable, and (D) secondary considerations. *Graham v. John Deere Co.*, 383 U.S. 1 (1966). Any differences between the prior art and the claims at issue must be such that they would have been obvious to a person having ordinary skill in the art at the time the invention was made. *KSR Int'l Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 1734, 167 L.Ed.2d 705, 75 USLW 4289, 82 U.S.P.Q.2d 1385 (2007).

Applicants respectfully submit that the present claims are not obvious in view of the cited references under a *Graham* analysis. More specifically, the combination of Lewis with Sudia fails to teach or suggest all of the limitations of claims 1-3, 5-24, 26-28, 50, 51 and 53-56, and one of ordinary skill in the art would not arrive at the limitations of claims 1-3, 5-24, 26-28, 50, 51 and 53-56 in view of the differences between these references and the presented claims.

A. Scope of the Prior Art

Lewis (U.S. Patent No. 5,761, 306) discloses a method in which a key server provides an active public key and a hashed replacement public key to nodes of a network. Lewis teaches that "the process of key replacement must occur both at key server 16 and at nodes 12, since the keys are paired. Thus, when the private key is replaced in storage 28, that replaced key cannot be used unless the public key stored in data storage 20 is also replaced." (col. 7, lines 50-54). Each time a key replacement is performed, the server 16 sends a key replacement message that includes the replacement public key 150, the hash of the next replacement public key 152, and

digital signatures for the message 154, 156 to the nodes 12. (col. 7, lines 60-67, col. 8, lines 1-2). In particular, Lewis teaches that "[t]he entire key replacement message is digitally signed by both the active private key.Apr, and the private replacement key. Rpr." (col. 8, lines 3-5). "If both digital signatures verify message 42, the node replaces H(Rpu) with H(R1pu) and replaces Apu with Rpu. In this way, the active public key stored in storage 20 is replaced with the replacement public key...." (col. 8, lines 51-57). **Thus, Lewis appears to require access to and use of the active private key in order replace and use the replacement private key. In other words, Lewis teaches that the replacement private key cannot be used unless the public key is also replaced, and then teaches that the public key cannot be replaced without using the active private key.**

Sudia (U.S. Patent No. 6,009,177) discloses a cryptographic system and method with a key escrow feature for verifiably splitting users' private encryption keys into components and for sending those components to trusted agents. For example, Sudia describes an embodiment in which the device includes a chip that breaks the private key into several pieces and forms a share packet for each trustee or escrow agent designated by the user. (col. 18, lines 12-26). It appears to Applicants from the disclosure in Sudia, that the purpose of keeping the private key with the trustee or escrow agent in Sudia is to verify that the user device is a trusted device and to provide a signed certificate from the master escrow center to be used for communications between devices (see, e.g., col. 20, lines 26-35), and to allow access to the private key by law enforcement for the ability to intercept and decrypt communication to and from a particular user (see, e.g., col. 30, lines 5-19). Applicants are unable to find disclosure, nor has the Examiner identified any disclosure, in Sudia describing the output of one private key and the retention of another private key at the user device. Instead, the only existing private key for the chip is both transmitted to the plurality of different entities and retained stored on the chip for subsequent use by the user device after it is transmitted to the trustee or escrow agent. (col. 17, lines 62-63).

B. Differences Between Claimed Invention and Prior Art

Claims 1-3, 5-10, 14-18, 22-24, 50 and 53-56

Claim 1, as amended herein, recites in part "outputting the second private key from the mobile user device while retaining the first private key in the mobile user device, wherein

outputting the second private key comprises transmitting a plurality of shares of the second private key from the mobile user device to a plurality of different entities once, **such that the second private key can be re-created and used when the first private key is *inaccessible*.**"

As noted above, Lewis requires access to the active private key in order to use the second private key. In other words, Lewis requires use of the active private key in order to sign the key replacement message to replace the active public key with the replacement public key. Lewis further teaches that the replacement private key cannot be used without the replacement public key. Accordingly, Lewis suggests that the invention disclosed therein is incapable of using the replacement private key without access to the active private key for signing the key replacement message. Therefore, Lewis fails to teach or suggest "outputting the second private key from the mobile user device while retaining the first private key in the mobile user device, wherein outputting the second private key comprises transmitting a plurality of shares of the second private key from the mobile user device to a plurality of different entities once, such that the second private key can be re-created and used when the first private key is inaccessible."

Furthermore, Applicants assert that Sudia fails to remedy these deficiencies of Lewis with respect to independent claims 1, 14 and 22.

Applicants respectfully assert that Lewis and Sudia, when combined, do not teach or suggest at least "outputting the second private key from the mobile user device while retaining the first private key in the mobile user device, wherein outputting the second private key comprises transmitting a plurality of shares of the second private key from the mobile user device to a plurality of different entities once, **such that the second private key can be re-created and used when the first private key is inaccessible**," as recited in independent claim 1 and as similarly recited in independent claim 14, and these differences between claims 1 and 14 and the combined teachings of the cited references would not have been obvious to one of ordinary skill in the art at the time the invention was made. Applicants, therefore, respectfully request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claims 1 and 14.

Similarly, Lewis and Sudia, when combined, do not teach or suggest at least "retain the first private key and output the second private key as a plurality of shares to a plurality of different entities once **such that the second private key can be re-created and used when**

there is no access to the first private key," as recited in independent claim 22, and these differences between claim 22 and the combined teachings of the cited references would not have been obvious to one of ordinary skill in the art at the time the invention was made. Applicants, therefore, respectfully request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claim 22.

Finally, Lewis and Sudia, when combined, do not teach or suggest at least "a transmitter coupled to the processor to: output the second private key as a plurality of shares to a plurality of different entities once, **such that the second private key can be re-created and used when there is no access to the first private key**," as recited in independent claim 50, and these differences between claim 50 and the combined teachings of the cited references would not have been obvious to one of ordinary skill in the art at the time the invention was made. Applicants, therefore, respectfully request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claim 50.

Furthermore, the nonobviousness of independent claims 1, 14, 22 and 50 precludes a rejection of claims 2, 3, 5-10, 15-18, 23, 24 and 53-56, which depend therefrom, because a dependent claim is obvious only if the independent claim from which it depends is obvious. *See In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988), *see also* MPEP § 2143.03. Therefore, Applicants request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claims 2, 3, 5-10, 15-18, 23, 24 and 53-56, in addition to the rejection to independent claims 1, 14, 22 and 50.

Regarding dependent claim 10, Applicants additionally assert that the cited prior art references, when combined, at least fail to teach or suggest "preventing retransmission of the second private key," as recited in dependent claim 10. In particular, the portion identified by the Office Action in Sudia merely teaches limiting the number of times the device can be rekeyed, but does not teach or suggest preventing retransmission of a private key. Therefore, Applicants respectfully assert that dependent claim 10 would not have been obvious to a person of ordinary skill in the art at the time the invention was made considering Lewis in view of Sudia, and request that the Examiner withdraw the rejection of dependent claim 10 under 35 U.S.C. § 103(a) for this additional reason.

Claims 11-13, 19-21, 26-28 and 51

Claim 11 recites, in part, "receiving a second public key from the mobile user device, the second public key associated with the first public key, wherein the second public key has a corresponding second private key that is split into a plurality of shares that are sent to a plurality of different entities, where each share is sent only once and to a different entity, **such that the second private key can be re-created and used when there is no access to a first private key corresponding to the first public key**, wherein the first private key is disabled when the second private key is re-created and used for authentication."

As noted above, Lewis requires access to the active private key in order to use the second private key. In other words, Lewis requires use of the active private key in order to sign the key replacement message to replace the active public key with the replacement public key. Lewis further teaches that the replacement private key cannot be used without the replacement public key. Accordingly, Lewis suggests that the invention disclosed therein is incapable of using the replacement private key without access to the active private key for signing the key replacement message. Therefore, Lewis fails to teach or suggest "receiving a second public key… [having] a corresponding second private key that is split into a plurality of shares that are sent to a plurality of different entities, where each share is sent only once and to a different entity, such that the second private key can be re-created and used when there is no access to a first private key corresponding to the first public key."

Furthermore, Applicants assert that Sudia fails to remedy these deficiencies of Lewis with respect to claims 11, 19, 26 and 51.

Applicants respectfully assert that Lewis and Sudia, when combined, do not teach or suggest at least "receiving a second public key from the mobile user device, the second public key associated with the first public key, wherein the second public key has a corresponding second private key that is split into a plurality of shares that are sent to a plurality of different entities, where each share is sent only once and to a different entity, **such that the second private key can be re-created and used when there is no access to a first private key corresponding to the first public key**," as recited in independent claims 11 and 19, and as similarly recited in independent claims 26 and 51, and these differences between claims 11, 19, 26 and 51 and the combined teachings of the cited references would not have been obvious to

one of ordinary skill in the art at the time the invention was made. Applicants, therefore, respectfully request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claims 11, 19, 26 and 51.

Furthermore, the nonobviousness of independent claims 11, 19 and 26 precludes a rejection of claims 12, 13, 20, 21, 27 and 28, which depend therefrom, because a dependent claim is obvious only if the independent claim from which it depends is obvious. *See In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988), *see also* MPEP § 2143.03. Therefore, Applicants request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claims 12, 13, 20, 21, 27 and 28, in addition to the rejection to independent claims 11, 19, 26 and 51.

New Claims 57-68

New independent claim 57 recites "re-creating a second private key **at a mobile user device that has no access to a first private key** associated with the second private key, wherein the second private key is re-created using at least some shares of a plurality of shares of the second private key located at a plurality of different entities; creating a third private key and a corresponding third public key; and **using the second private key for authentication of the mobile user device**." Independent claims 61 and 65 also include similar recitations.

As noted above, Lewis requires that a device has access to the active private key in order to use the second private key. In other words, Lewis requires use of the active private key to sign the key replacement message in order to replace the active public key with the replacement public key. Lewis further teaches that the replacement private key cannot be used without the replacement public key. Accordingly, Lewis appears to be incapable of recreating a replacement private key at a mobile user device that has no access to the active private key, and using the second private key for authentication of that same mobile user device having no access to the active private key. Therefore, Lewis fails to teach or suggest "re-creating a second private key at a mobile user device that has no access to a first private key associated with the second private key…; and using the second private key for authentication of the mobile user device."

Furthermore, Applicants assert that Sudia fails to remedy these deficiencies of Lewis with respect to independent claims 57, 61 and 65.

Accordingly, Applicants assert that new claims 57, 61 and 65 are allowable over Lewis and Sudia. Applicants further assert that each of dependent claims 58-60, 62-64 and 66-68 are allowable at least by virtue of depending from allowable base claims.

Should any of the above rejections be maintained, Applicant respectfully requests that the noted limitations be identified in the cited references with sufficient specificity to allow Applicant to evaluate the merits of such rejections. In particular, rather than generally citing whole sections or columns, Applicant requests that the each claimed element be specifically identified in the prior art to permit evaluating the references.

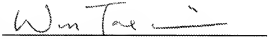
CONCLUSION

In light of the amendments contained herein, Applicant submits that the application is in condition for allowance, for which early action is requested.

Please charge any fees or overpayments that may be due with this response to Deposit Account No. 17-0026.

Respectfully submitted,

Dated: June 28, 2010

By: 

Won Tae C. Kim, Reg. # 40,457
(858) 651 6295

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121
Telephone: (858) 658-5787
Facsimile: (858) 658-2502